THE BROOKINGS INSTITUTION

CYBERSECURITY AND CYBERWAR:
WHAT EVERYONE NEEDS TO KNOW - AND HOW TO TALK ABOUT IT

Washington, D.C.

Monday, January 6, 2014

Panel I: What Everyone Needs to Know:

NOAH SHACHTMAN
Executive Editor of News
Foreign Policy

PETER W. SINGER
Co-Author, *Cybersecurity and Cyberwar*
Senior Fellow and Director, Center for 21st Century Security and Intelligence
The Brookings Institution

ALLAN FRIEDMAN
Co-Author, *Cybersecurity and Cyberwar*

Panel II: How to Talk About Cyber:

NOAH SHACHTMAN
Executive Editor of News, *Foreign Policy*
Nonresident Senior Fellow, The Brookings Institution

SIOBHAN GORMAN
Intelligence Correspondent
The Wall Street Journal

DAVID SANGER
Chief Washington Correspondent
The New York Times

JAMES BALL
Special Projects Editor
The Guardian

TOM GJELTEN
Correspondent
NPR

* * * * *

P R O C E E D I N G S

MR. SHACHTMAN: Hi, everybody. I'm Noah Shachtman, I'm a non-resident fellow here at Brookings and I work for a magazine down the street called *Foreign Policy* and I'm really honored and I'm really excited to celebrate the launch of Pete Singer and Allan Friedman's really interesting book, which I have right here in my hand, *Cybersecurity and Cyberwar: What Everyone Needs to Know*, which has already been endorsed by everybody from the former commander of NATO to the head of Google to the producer of *24* and *Homeland*.

And we're going to talk today about some of the big issues in cybersecurity, sort of what are the policy implications of them, what are the policy responses, and what can we do as ordinary folks.

Peter, as I'm sure you all know, is director of the Center for 21st Century Security and Intelligence here at Brookings. Allan is now a visiting scholar at the Cybersecurity Policy Research Institute at George Washington and was here at Brookings for three years.

And it's interesting to me that, you know, just to kick things off, that this book is coming out now. I mean, we've sort of had, it seems, like a stream of cybersecurity stories, mishaps, events, in the last, you know, five years, and so I guess I'm curious why you guys decided now was the time to sort of in a way kind of go back to basics and set the table and kind of lay out a primer for folks about what they needed to know on the topic.

MR. SINGER: I'll weigh in on that and first want to thank you and thank all of you for coming out. Really appreciate it. It's an exciting time for us and that actually links to your question because a book is a journey, you know, it's coming out right now, but it's showing the journey of almost two years, and the idea behind it, and why we think it's particularly relevant right now, is that I would argue there's no issue that's become more important, that's less understood, than cybersecurity.

And when I say “more important”, more important in terms of its policy implications, whether you work on classic military issues, national security issues, to legislative questions, to the business side, to your own role as a netizen, but also at a citizen or a parent. Another way of putting it is that the issues that are at play here are as weighty as the future of world politics, to as important as your own personal privacy or your kids on what they’re doing on Snap Chat or the like, and yet there’s a gap there and the gap we can see it in lots of different ways. We can see it in the former director of the CIA described it as he’s never dealt with an issue where there was less knowledge among the people around the table making decisions to 70 percent of business executives have made a cybersecurity decision for their company, not 70 percent of CTOs or CSOs but of execs in general, and yet no major MBA program teachers on it as a regular management issue to, again, you know, our own personal -- the way we handle our self online in terms of, you know -- our favorite story is probably the most popular password is still password, followed by 1-2-3-4-5-6, which is, you know, the joke was that that’s what I use on my luggage.

But also, again, to how we handle a citizen, all these different issues that are popping up right now, whether it’s the NSA or the like, and so the goal behind the book was to -- as you put it -- get to basics. I would argue, though, it’s not back to basics because we never got to basics in the first part, and so it’s to give you an easy to read primer of all the key questions, everything from how does this all work to why does it matter to, finally, what can we do about it, and to do it, and again, emphasizing what everyone needs to know, because as long as we have the Internet and we’re using it, we’ll have issues of cybersecurity and cyber war.

MR. SHACHTMAN: Allan, it seems to me 2013 was kind of the -- was the year of the leak, right, I mean, in terms of cybersecurity. I don’t know if you guys heard, there was an NSA contractor who got his hands on some documents.

What do you see 2014 heading? What’s the text landscape like? What are the big issues we're going to face? What's 2014 going to be the year of?

MR. FRIEDMAN: You know, the nice thing about predicting the future is you can say it's going to be like the past, but more so.

MR. SHACHTMAN: Yeah.

MR. FRIEDMAN: So, looking back, one of the interesting things about 2013 was I think it was the first year that no major person in the policy world gave a speech that amounted to "the problem with the Internet was that it was built without security in mind; the solution is therefore to build a whole new Internet, but this time we'll make it secure".

MR. SHACHTMAN: Right.

MR. FRIEDMAN: So, we're starting to move in this direction, but ultimately we want to move from an area where cybersecurity is something that is seen as unique and separate and cut new out of whole cloth into an issue that is now integrated into everything, where the manager can't just say, I'm going to call my cyber guy, you're going to have to have cyber people involved.

So, one thing I think we can expect to see is boards of directors are going to start demanding briefings. They're going to say, listen, we hear about this stuff, how are we covered? At the technical level, you're going to see a lot more creative attacks where we're going to move from just taking advantage of the human error and finding new challenges.

One of the largest questions is -- are always at the sort of intersection of the technical and the economic and political, so who bears the responsibility for security your cell phone? Is it the manufacturer of the phone? Is it the manufacturer of the operating system? Or is it your cell phone company with whom you have a direct relationship?

I think in 2014 those questions are going to come to a head and we're going to see a lot of lawsuits and we're going to see a number of people trying to propose new technical fixes. The challenge is going to be to make sure that we don't fall for snake oil and actually work towards a sort of coordinated approach.

MR. SHACHTMAN: And I'm going to ask a couple more questions of these guys because there's some things I'm dying to ask them, and then we're going to open it up to the audience, so get your questions ready.

You know, both of us have sort of worked around Pentagon types for a while and it always seems like the answer to any cybersecurity question is, like, more offense, like, you know, and you know, if we're being hacked, the answer is to hack them back 100 times more.

First of all, do you see that trend continuing in the government that everything's got to be about offense? And secondly, does that trend so far make any sense?

MR. SINGER: It's a good question and it's a big question of consequence when we think about not just what we're spending on, but the potential of this to spiral out into directions that we don't want it to or we lose control over.

And, you know, so this notion of cyber offense is very appealing, it's appealing in terms of just how it sounds. If somebody attacks me, I'll attack them first; or the best way to defend yourself is a good offense. We can see it and its implications in the assumptions that we're starting to bake into our military doctrine that's out there. For example, there was a Pentagon statement that says that in cyber space that offense will be dominant "for the foreseeable future", that's the Pentagon's assessment.

There's a series of issues with that, the first is actually cyber offense, a true cyber offense, an effective one, a Stuxnet style -- you know, in our next panel we're going to hear from some experts on it, but to do something like that is quite difficult, it's not as we've seen senior Pentagon officials describe where they -- you know, they're phrasing it is that a couple of teenagers -- and this is their quote -- sipping Red Bull, wearing flip flops in their parent's basement could pull off a weapons of mass destruction style event. No, they couldn’t.

There’s very real -- and, you know, we wrote a book on it -- very real cyber threats out there, but to do some of the more effective stuff, it’s not that easy. Also, the defender actually has a series of steps that they can take to make cyber offense difficult. But what I’m getting at is that it’s not this easy offense way.

The second is when you start to connect both the technical side to the military side to the policy side to the history side, you see some lessons crossing back and forth. So, for example, every time in military history where someone has said that the military offense will be dominant, actually history had a great way of teaching them that it played out the opposite. Prior to World War I would be a really good example of this.

The next problem is, where do these assumptions sometimes take you? And we’ve seen this in what we’re spending on right now, the U.S. military is spending -- it depends on which study, but roughly 2.5 to 4 times as much on cyber offense research as they are on cyber defense research, which one has certain implications for a kind of instability, but also if you go back and, you know, connect to security studies, it’s a lot like thinking that the best way to protect your house, your glass house, from a gang of roving teens is to buy a stone sharpening kit. And that’s, you know, the implication here. We need to come to a balance not only in how Allan was talking about -- saying of how we talk about, how we assess these threats, but also a balance in what we’re spending on and how we approach it.

MR. FRIEDMAN: And just from a political perspective, one of the things that I think is a novel aspect of this from an international conflict perspective is when we talk about attacking their systems and they talk about attacking our systems, they are the same systems. We are using the same platforms, and so often we are going to be faced with a decision of do we exploit the other guy or do we work towards defending ourselves. And when you start to realize, well, actually, there’s not just us versus them, it’s us defined many different ways and a whole lot of different thems. You need to have some kind of equilibrium where we tip towards the defense, where we emphasize the fact that we’re all better off if we move towards a more secure posture.

MR. SHACHTMAN: Yeah, and we’ve seen that in the NSA story, right, which is I think one of the reasons why a lot of people are outraged is that they’re not just undermining, you know, accessing the email accounts of a couple of terror suspects, but they’re sort of undermining some fundamental security protocols that work for all of us.

MR. FRIEDMAN: I think that’s a key point. So -- and we don’t want to over state it, right, so there was a headline in the *Washington Post* this weekend that said, you know, the NSA is trying to break all of our codes. Well, that’s kind of their job, right, their job is to be a foreign intelligence organization.

The challenge is, how are we going to scope it and how well is this playing with other national priorities? And we want to make sure that other national goals for diplomacy, for commerce, for trade are balanced in the government’s process, and I think that’s why a lot of Americans were very upset and why people around the world said, well, you know, what does this mean for us? If we have the power to do this, shouldn’t we be doing this as well? That doesn’t lead to a very stable world.

MR. SHACHTMAN: Peter, how do you think -- well, I’ll just speak personally -- is that I think pre-Snowden in -- you know, I had some -- I was doing some policy work here and frankly it relied on trust in the government that I feel like I can’t take anymore after the Snowden leaks. Maybe you can talk to me a little bit about how those leaks are kind of effecting policy prescriptions across the board.

MR. SINGER: Well, I think the challenge of what was disclosed is the massive scale of it brought together a variety of things, and so when we’re talking about the leaks, I categorize them into sort of three types of activity, the first was smart, sensible espionage against American enemies. There’s a series of activities that were disclosed that way. The second category I would put in terms of “questionable” -- legally questionable, politically questionable, basically efforts that involved U.S. citizens through some way, be it by a fuzzy legal definition, a technical back door, using a foreign effort, but basically it's the category of questionable.

And to be blunt and direct, a third category that we could call "unstrategic" or "stupid", which is collecting intelligence on close American allies. And the challenge is that we have these three categories that are out there and so when people talk about this issue and how either upset they are about what the government's doing or upset they are with Snowden and should he get clemency or not, they usually kind of focus in on one of those categories.

And in turn it's also effected the way we talk about it and we've defended these programs in public where much of what matters in the U.S. political discourse is category two, the legal questionable stuff, but saying we're doing that to prevent another 9/11 doesn't make Angela Merkel and the Germans feel better about it because they're in category three.

And the real effect of this, I think, is not just in terms of how it's changed the political discourse here, but the long-term impact of it is probably most going to be felt, I would argue, in two ways: one, on American business, particularly technology companies, which at least according to a report from Forrester, will lose as much as $180 billion worth of revenue because of disclosures around these activities. That's why they're so peeved.

The second is -- and it goes to one of these 2014 questions, is the ongoing debate over the future of the Internet itself and its governance, which, you know, in the book we talk about these issues and looking at the ITU -- well, these questions around Internet freedom, and frankly, kind of the Internet freedom agenda that the State Department has been pushing, kind of feels almost dead right now. We've sort of lost our swagger.

And in the year ahead, there's going to be some big decisions to make and my worry is that it's a combination of us losing our swagger on Internet freedom issues combined with we may have lost certain key swing states that were with us previously and so my fear is that if we don't watch out in the year ahead, the Internet that all of us have kind of grown to know and love, will not be the ones that our kids inherit.

MR. SHACHTMAN: And that's because of why? Explain that.

MR. SINGER: It's the idea that there's very different visions about the Internet and how it should be governed, so to speak, and what should be the role of states versus the kind of multi-actor layer of responsibility, kind of weirdly but wonderfully informal setup that we have right now that's worked so well, and we're particularly seeing this being pushed by authoritarian states. So, another way of putting it is, if you like the way that Russia blacklisted 82,000 websites -- when you try and -- you enter an address and it doesn't go to where you want, that very much could be the future if we don't watch out.

That's different than the NSA worry that you talked about, which is the monitoring side. It's two very kind of different state problems, but in the politics of it, they've gotten wrapped together.

MR. FRIEDMAN: And that's exactly right, they've been tied together, so you have sort of genuine concern about the process that Peter mentioned, that sort of very ad hoc, which, I think, to be fair, does seem to hue closely to American interests. We sort of set up this organization, ICANN, and it works well, although if you look at the organizational structure on paper from a political perspective you say, well, that's not fair, and let's move to a more representative style, where every country gets a vote the same way we have the UN, and the problem is, while that may sound good from an organizational perspective, it may sound equitable, the consensus seems to be it's going to really empower two types of countries, those that want to throw up barriers around their own national networks for national security reasons, how they define their own national security, and countries that want to throw up barriers around it for economic reasons, they want to sort of go back to sort of a local tel-com monopoly style.

And this discussion has been sort of really pushed. Last December in 2012 it came to a head at a conference in Dubai and the United States and its allies, including Brazil, really held off this. We lost the vote but maintained enough to keep the status quo working.

And I think if that vote had been taken shortly after the Snowden leaks, I don't know how many European allies would have voted with America. So, I think the real risk of a balkanized Internet, where each country sets up its -- not only just its own policies at the network level, but may actually say, well, listen, we want to make sure that our technology is in the network and in the computers. We're going to have national level policies about what kind of crypto-algorithm you can use or how you store your data. That means that everyone who's making this technology now needs to make a separate chip for each country, and that really is going to hurt the pace of innovation and sort of change how the whole cyberspace evolves.

MR. SINGER: There's two more things to add on this. On the domestic side, the sort of link to classic cybersecurity questions, and one is what this has done to, you know, the politics of cybersecurity on Capitol Hill where, you know, look, we haven't had major cybersecurity legislation pass since 2002. That's five years before anyone heard of the iPhone, and because of this and a number of other factors, it'll be another year at least before we get anything around it because we've got this whole other bundle of questions that it just got tied into.

The other goes back to your original idea of trust and it's trust in the computer labs and in Silicon Valley, which, you know, I met with a senior leader at a Silicon Valley company who described that they felt they were now in an arms race with their own government, with the U.S. government, and the same when it comes to -- you know, in the book we talk about the importance of finding the "IT" crowd, finding the IT folks, you know, how do we deal with this human capital problem in cybersecurity? Well, now some of our government agencies have a major issue here at the same time where we need to do a better job of recruiting cyber talent, you know, by one measure, we're only getting around 10 percent of the cybersecurity professionals that we need. Well, now it's going to be even more difficult because of, you know, kind of the tenor around this topic.

MR. SHACHTMAN: I'd like to take some questions from the audience. Please phrase them in the form of a question, not a rant, statement, or diatribe. That means have a question mark at the end or have your voice turn up at least at the end. Start here in the front.

MR. PAYNE: I'm Jim Payne with a local contractor/vender, Z&A. I want to pull the thread on Internet governance. It's been said that this is as much of a threat as a physical attack on the Internet. So, my question is this, with a question mark, where in the administration does this issue about Internet governance reside? Who sets that policy? Many people believe that the current ICANN model is too U.S.-centric, so as we need to evolve, where in the administration -- what organization, agency -- does this reside?

MR. FRIEDMAN: So, like a lot of cyber issues, really covers a lot of ground because the question of Internet governance covers everything from how do we get new domain names or new top level domain names, so we're moving from a world where everything was either a .com or a .uk, to now anyone can propose their own domain name -- that's a trademark issue -- versus the very real questions about how do we secure that domain name system or how do we allocate the remaining IP addresses, because we're running out of them. And those cover very different issues.

Traditionally, you probably know this, this has been in the Department of Commerce, which has the contract to negotiate what is called the root, which is the head of the Internet in the domain name system. We talk about this further in the book, there's even a nice graphic to help you understand it.

What past administrations have been very successful in doing, as well as ICANN, is working to make sure this isn't purely an American question, but at the same time, the organizational questions of who is going to be in charge globally is a question of international diplomacy where people are lobbying on either side, and that's predominantly residing in the State Department.

MR. SINGER: Let me add, part of the challenge when it comes to the policy and the strategy here is two key words: ignorance and imbalance. Ignorance, senior policy makers, the people who truly can make decisions, are not well equipped to deal with these issues, and we've got, you know, all of the wonderful, great anecdotes in the book on this, whether it's a senior diplomat about to go negotiate with the Chinese on Internet issues who asked us what an ISP was, which is a lot like going off to negotiate with the Russians in the Cold War and not knowing what an ICBM is.

And, you know, look, I'm kind of mocking this but my mom also doesn't know what an ISP is and does know what an ICBM is even though, you know, one's clearly more important -- my mom was a nurse -- to the former Secretary of Homeland Security who proudly talked about the fact that she hadn't used email or social media for over a decade because she didn't think it was useful.

We could go on and on with all these examples. So, you've got that level of kind of ignorance and, you know, it's just there, but the imbalance side is also there. It's there, and when we talk about the threats, you noted, you know, this may be as bit a policy issue as there is, and yet that's not talked about. When it comes to actual -- the notion of kind of cyber attacks, as opposed to a structural problem, you know, I would argue that the massive campaign of intellectual property theft that's going on against the U.S. right now, you know, maybe as much as a trillion dollars worth of value lost, that matters far more than the narrative that's out there, a half million times we've talked about cyber 9/11 or cyber Pearl Harbor or the 31,000 news and magazine articles that have been written about cyber terrorism, despite the fact that no one has actually been hurt or killed by cyber terrorism.

In the book we joke that it's a lot like Shark Week, you know, where we obsess about sharks even though you're 15,000 times more likely to be hurt by your toilet. The reality, though, is that a shark has actually hurt someone unlike cyber terrorism.

The power grid scenario, squirrels have taken down the power grid more times than the zero times that hackers have. So, we've got this imbalance in the threat, but also to how we structurally respond to it, whether it's our spending when it comes to budgets and kind of the more focus on certain agencies, to the decision making question.

In the White House you've got 12 people on the National Security staff at the NSC working cybersecurity questions. You've got one on the economic side who also, by the way, has responsibility for things like copyrights, et cetera.

So, you know, we very much need an approach that's both informed and balanced.

MR. SHACHTMAN: Next question over here.

MR. DOWNEY: Thank you. Richard Downey from Delphi Strategic Consulting. Thank you for a very interesting discussion.

You mentioned a little bit about corporations and how they are protected or how well they are or are not protected and, you know, intuitively you would just assume that large corporations or banks that have lots of resources would do what was required to protect themselves against these kinds of threats, and I've seen this -- it's a cybersecurity maturation model that measures how prepared either organizations or countries are against these kinds of threats. It's essentially an X-Y axis, zero starting as defenseless and the curve goes up to resilient, which is if you get an attack you can defend against it easily.

And I wonder if you could talk about just in general how along that curve, how prepared you have found corporations and banks to be in preparation against these kinds of threats.

MR. FRIEDMAN: I think the spectrum you're referring to is the World Economic Forum's Resilience Spectrum. Is that the one you're talking about?

MR. DOWNEY: (off mic)

MR. FRIEDMAN: Okay, sure. So, there are a number of approaches like that. You know, it's funny that you used banks and major corporations because I think that helps us understand the issue a little bit. Probably the leaders in both developing defenses and working together to understand how the rifts are interconnected is the financial sector. Why? Because the financial sector faces very real loss threats from criminals.

You know, why do you go after banks? It's where the money is. And so the financial sector has learned to work together, develop good defenses, and also understand it from a risk perspective. They don't have to stop every single attack. They have some models to understand the relationship between how much to invest and what they get out.

Most companies, in the broader economy, don't have that. Now, they don't have that for a number of reasons, one, we don't have a good way of understanding what our losses, what our risks are. Often when we talk about the theft of competitive data, we usually think about "the Special Sauce". When Coca-Cola was hit in 2010, so -- an attack that was later attributed to the group that is associated with the Chinese government, did the bad guys go after the secret formula for Coca-Cola? No. No one really cares about that. What we do know is that less than ten days after the attack happened, the Chinese government rejected Coca-Cola's bid to buy the largest soft drink bottler in China.

Now, this was a bid that everyone on Wall Street thought would go through, so we have to think about what is at risk from a very broad perspective.

The challenge is actually understanding what is at risk and how to defend ourselves and that's a really big job because it involves having a holistic view of what's at stake in an organization. That has to come from the board top down, and it also has to come from thinking about the risks we face in a way that the managers and the board will say, well, listen, we have real immediate losses that we can tie to failure to act now and that may come from the market, it may have to come from a more interventionist government approach.

MR. SINGER: One of the main lessons of the book is that, as opposed to how this is often framed and talked about, this cybersecurity, this problem area, whether you're talking about at the national level all the way down to you as an individual, it's not about the software, it's not about the hardware, it's about the wetware, it's about the people, it's about the incentives that drive them, the organizations that they're in, the level of awareness. It's all about the people at the end of the day.

And in turn, in your question, you used a really important word, which was "resilience" and one of the things we very much push is the idea of a resilience model rather than this kind of discourse that's sometimes out there of, you know, someone that has the secret sauce solution for all your problems or I can hack back and it'll solve all the problems or, no, all we need to do is build up a Maginot Line kind of defense. I mean, you see that. No, it's about resilience.

And the idea is, you know, resilience, whether you're pulling from the resilient human body or resilient when it comes to psychology, it's the idea that bad things are going to happen, it's how you bounce back from them. Your body doesn't just have an exterior layer of defense and it's penetrated and, oh, that's it. I got cut; it's over.

Your body is set up to do everything from isolate that, to it can triage, figure out what's important, what's not, it recovers. If we're thinking about the psychology side, resilience -- you know, you can't go through life thinking that no bad things are going to happen. A resilient mentality, a resilient relationship is something that can deal with the bad things and recover and yet, again, to go back to what we were talking about before, part of the problem of how and why we've talked about cybersecurity issues is, you know, we joke, we turn the volume up to 11 *Spinal Tap* style. Get scared! And I've got all the solutions for you. And, you know, the power grid scenario.

I guarantee you, someone is going to lose power in the Washington, D.C. area in the next 48 hours. But if we put the word "cyber" in front of it, we would suddenly have Congressional panels going, "Who's to blame?" "What's wrong?"

MR. FRIEDMAN: And a lot more money to fix the problem.

MR. SINGER: Yeah, and that's part of it. So, you know, resilience is the model that I'd prefer us to have rather than where we're at now. And resilience, again, whether you're talking about the nation, down to you as an individual and how do you protect, you know, you're cherished memories and files. You ought to be thinking about that for yourself.

MR. SHACHTMAN: Let's go here.

MR. BEREEN: Thanks a lot, gentlemen. Andrew Bereen. I'm an attorney here in town. I focus on national security, humanitarian law, and do some work with Truman National Security Project on cyber initiatives and defense work.

My question is, we talked a lot about the problems, right, I think the NSA is a pretty easy whipping boy, there are problems with corporations not taking their own initiative, but on the opportunities for leadership and the opportunities for government policy to move things forward, in the absence of legislation, President Obama signed an executive order on cybersecurity with the NIST framework incorporated into it, and I'm wondering what the three of you actually think or hear about its prospects for actually helping enhance the resilience and security posture of the U.S. nation. Right, we're not talking about global security, just start with U.S. nationals, U.S. interests. Does that executive order move us closer and move us in the direction we need to go in the absence of legislation?

MR. FRIEDMAN: So, the core, for those of you who don't know -- the core of the executive order is to develop a voluntary framework to implement existing standards for more security. So, this applies to all of critical infrastructure, which is legally defined but we usually think of it as sort of the basic essentials, you know, light, air, water, things like that.

The challenge of this framing, you know, we can think of the government as being good at some things, like hitting people with a stick to get them to do things, and bad at other things, like developing technical standards, and one way to look at the executive order is to say, well, we've sort of flipped that. Government is collecting all the technical standards, but there's no enforcement tool. So, that's why a lot of people are skeptical.

I think there is some reason to be optimistic for a number of reasons. One, NIST has really succeeded in getting the right people in the room to start paying attention. Representatives from all the major industries have stood up, they're watching what's going on, they're trying to figure out how do we get ahead of this.

The notion here is that this is the sort of last opportunity that industry has to fix the problem themselves, and so if we think of the executive order as a "do it now", and I've got the stick of regulation behind my back, and in fact that's part of the executive order is to identify areas where this isn't working. So, that's one reason to be optimistic.

Another approach is really we do need to have a rising tide lift all boats, so we need to find the tools to get various players to work together and it provides a platform and an organizational venue for different parts of complex supply chains to get together and talk about how their risks are interdependent.

So, that sounds fluffy, or even worse, it sounds boring, but that's really where we want to be. Cybersecurity shouldn't be this sexy, new thing. Cybersecurity should be the boring work of lawyers talking to other lawyers, economics talking to other economists, technologists talking to each other, and having everyone talk to each other, lots of conversations so that everyone is on the same page, and hopefully we keep turning that page and getting a little better.

MR. SHACHTMAN: Allan, just a quick book sales note, I'm not sure you want "cybersecurity is boring" to be a tagline.

Let's go to another -- Jim?

MR. HANSON: Jim Hanson from APPSIO. I had a question. Historically, information security has focused on the perimeter. You know, you build bigger walls around the data; you make sure that nobody can sneak in and hack your data. Bradley Manning was an insider authorized access. Between him and Snowden, we obviously did not make a whole lot of progress.

When people -- you know, the major breaches and leaks we've had, no one backed a panel van up to a data center and took off with all the servers. People are stealing data. Have you seen any advances or a move beyond perimeter security to look at what they're actually stealing, the data itself, and that as a focus?

MR. SINGER: I'll jump in on this one and then you can do as well. You hit it exactly right, this mentality that if we're making a military parallel, it's Maginot Line thinking or it's, you know, the walls of Jericho. Walls never work.

Frankly, it's the same, to go back to this issue, the past question of infrastructure, you'll sometimes say, well, I don't need a wall, I just won't link, I'll have an air gap. You know, I liken air gaps to those balloons that the nuns would try and put between the teenagers at catholic school dances. You know, they just don't work in the end.

You know, the Iranians thought they had a wonderful air gap defending -- keeping, you know, bad malware out of their nuclear research. Didn't work for them.

And so, instead we have to change -- you know, I was talking about this resilient model, but also, you know, following basic measures in terms of not only trying to keep bad out, but monitoring what's happening on your own networks, including by your own people, and whether it's the Manning episode or Snowden, those organizations, as sophisticated, as well-funded as they were, the U.S. military, the NSA, they were not following basic rules and procedures that a cupcake store should have.

The same when it comes to, you know, the power of very basic cyber hygiene, you know, the most important penetration of a U.S. military network, you know, by an outsider, happened because a solider found a memory stick in a parking lot and thought it was a good idea to plug it into their computer.   That's not just cyber hygiene, that's basic hygiene, that's the five-second rule, and it carries across this.

And look, we're laughing, but there's the same story of a major technology company was hit when someone -- a guy picked up a CD that he found in the men's room. Would you pick up anything you found in a men's room? A piece of food, a comb, or whatever, and plug it in, take it home with you? He did it with a CD. To all of us who work in the policy world, go to conferences where you're given these memory sticks out as favors, I mean, but what I'm getting at is, very basic hygiene -- and it goes back to this notion of the past question of the standards, you know, the top 20 controls, at least one study found that they would stop 94 percent of all attacks. Ninety-four percent.

And we go, well, whoa, what about the other 6 percent that might come from someone sophisticated, by an APT. Well, I hate to tell you, but all of you are not being targeted by APTs.

The second is, even if you are -- an Advanced Persistent Threat, you know, someone -- a sophisticated operation. Even if you are, go talk to your IT folks. They would say, if I didn't have to spend 94 percent of my time running down the low level stuff, I could focus on the advanced stuff.

And then finally, guess what, the advanced stuff often gets in through these low level things. You know, my favorite recent story of this was diplomats at the G-20 conference who got spear-fished, so to speak, by -- they received emails that led them to click on a link where they thought they were downloading nude photos of the French First Lady and instead they were downloading spyware.

I mean, we could go on and on with these stories, and so if we could solve these very kind of basic levels, we could do a lot better and then get to some of the more sophisticated technologic responses.

MR. SHACHTMAN: Anybody else have a question about picking things up in the bathroom? There in the back. Yeah, you.

MR. SINGER: I'm using these, in part, we have to stop talking just in kind of Cold War frameworks, which is the main way this is talked about in this town or it's just like a WMD, which has been said by everything from national security advisors to Senators, like, if we're going to be using metaphors and comparisons, the period of the Cold War is not the only one to draw from. And in fact, if we're drawing from the Cold War, to me we're in the period of the early stages of the Cold War where we didn't understand the technology, but we also took *Dr. Strangelove*-like characters seriously.

SPEAKER: Not exactly about hygiene. My name is Saleem. I'm a student at SAIS across the street. If you zoom out a little bit and think of the world, I mean, people talk a lot about the U.S., Russia, China, but very few people talk about sort of the tier down, which is, I think, countries like Israel, the EU, and then there's another tier down, which is I guess Latin America, maybe Central Asia.

I mean, I come from Turkey where a recent government report said that very sensitive information was protected by passwords like 1-2-3 and very weak systems.

What do you think is the place of those countries, the sort of lowest tier in cybersecurity in the future?

MR. FRIEDMAN: So, there are a number of different issues there. So, for example, the number one generator -- according to ACAMA, the number one generator of malicious traffic on the Internet right now is Indonesia. So, how did Indonesia get to be this (inaudible), which is also interesting, but we've seen this, this is now a real issue for every country.

Now, there are some benefits to being small. You actually can have a trusted group of people, so I know we've chatted here at Brookings with some governments that have been the victims of cyber attacks and they set up a -- sort of a voluntary -- volunteer army to sort of react in case of crisis, and that works at a small country, that would never work in a large country the size of the U.S. or China.

But there also is a very real danger of what I call cybersecurity ghettos, where as more and more countries develop the basic defenses, you're going to have those who are seeking to exploit insecure infrastructures move to a smaller and smaller set of countries that then have a much higher bar to make themselves more secure.

And so the downside of I don't have to outrun the bear, I just have to outrun you, is you've got a number of people who just are slower and I worry we'll be the sort of source of attacks.

Now, this has been identified as an issue. In fact, the Republic of Korea has said, listen, cybersecurity capacity building should be a priority for the World Bank. And they're trying to figure out how they can go about building that kind of international cooperation to really raise everyone up at least above a minimum level.

MR. SINGER: One of the other things, and you touched on it, is this is a space where you have so many different types of players, and in this question response we fell into that old kind of political science flaw of just talking about states, and yet this is a domain where everything from states large and small to non-state actors that range from targeting Google to Anonymous to you and I all matter, we all play, we all have power, different levels of power, but we all matter in this and so if we're talking about, you know, problems and solutions, we have to move out of that sort of classic framework.

And that leads to, you know, one, back to a policy side, we can draw lessons from other actors out there. So, as an example, there is an active debate within the U.S. military right now about what's the role of the National Guard and Reserves when it comes to cyber, and we're approaching it in a very classic National Guard and Reserves model versus, I think, Estonia's model. Its Cyber Defense League offers a lot of interesting things to draw from that might be far more effective.

Similarly, if we're talking about the makeup of the Internet itself is fundamentally shifting, the location of the threats to, you know, the anecdote that we use to illustrate this of, you know, how the Internet is changing, is that if you look at Google tracking, cute cat videos are now starting to lose out to cute panda and cute goat videos. It's a fun way of showing the power of Chinese users of the Internet and African users of the Internet are growing, but also their cybersecurity, both threats and concerns, are growing with the number of videos that are out there.

MR. SHACHTMAN: How about here in the front?

MR. SILVER: Arthur Silver, unaffiliated, but I do have an ATM card.

How hard or easy is it to obscure or, indeed, to forge the origin of a cyber attack?

MR. FRIEDMAN: From whom? It depends on who you're trying to fool, right, if you're trying to fool your basic sysadmin, fairly straightforward. If you're trying to fool a national intelligence organization, you not only have to use technical obfuscation, you also have to have perfect operational security, and so you have to remember that, you know, among the defenses that countries have, is not just, let me look at this packet and try to use technical forensics, it's, let me see what my intelligence service, as they've been eavesdropping on satellite and phone calls, what are they telling me about it.

And so then you also have to narrow it down further to, who wants to attack you without you knowing it was them, which is also a much smaller set of people.

So, it depends on what kind of attack you're worried about and what kind of resources it is. So, if you're trying to fool your local police department about who is sending all the money in a bank account to Kazakhstan, pretty straightforward. If you're trying to fool the federal government into a false flag operation, you need to do it a lot more carefully and it's much, much harder.

MR. SINGER: But you made a joke at the start about your ATM card, but it's a great illustration of some of the earlier points, the first is, you know, your ATM card, it's a multifactor approach to security. It's something you have, but then they also ask you for something that you know, your password, and that points to two things, first it points to why does the bank have that structured as opposed to, you know, the way we approach security maybe in other sectors, and it goes back to what Allan was saying of the differences of incentives in different kinds of industries, where banks, because they understand the price, and, oh, by the way, there's a legal framework that drives that kind of price for them, they've put in those kind of security requirements that you think are quite simple and easy, versus a power company that doesn't have these kind of approaches and still does use, you know, the 1-2-3-4 password approach or the 80 percent of small power companies that aren't under any kind of cybersecurity regulation right now.

And so, to me, it points to this value of the incentives, but also how personally we should all be thinking about our own security. So, you have that multifactor for your ATM. Do you have it for your Gmail? If you don't, you should.

MR. SHACHTMAN: We've got about 10 minutes left in this panel and then we're going to roll right into our next panel with some of the top reporters in DC and New York who have assembled here today. So, let's do two more quick questions and then we'll roll into our next panel. Over here.

SPEAKER: Hi, I'm (inaudible) from the Dutch embassy and I like it very much that we have the conversation about the human factor of the Internet because the Internet space domain is getting extended to not only our digital nations, but also our human nations.

But I want to talk about the last 6 percent where a role for government could be -- yeah, could exist. So, I want to give you three examples and I want to ask your opinion about it.

The first one are the black markets of the Internet. Actually, one of the main drivers or one of the main successes of the Stuxnet is the use of zero-day exploits and I think there is -- well, there's a role for government here and another example is the industry leading processes in chip manufacturing. The underlying assumption is that cryptography is -- cryptography does not lie only in software but also on hardware, and breaking these cryptography on a hardware level can have an origin in our industry and, hence, our government has a role in that.

And the last example is about ISP. I've seen a professor doing a huge research on the role of ISP in combating botnets and these are responsible for spam and/or spyware version that arrives on our Blackberries of the G-20 congress. So, how do you think about these three examples with respect to the government's role?

MR. SINGER: I'll try and jump on them real rapidly given the time that -- first, on the black market, it's a very good illustration of the lessons to be learned from both contemporary security policy as well as history, not just sort of within the cyber domain. So, if we're thinking about current counterterrorism policy, playing whack-a-mole is a loser's game versus going after the underlying structures. It's the same thing if -- and the book -- and Noah's also written about this -- of understanding the parallels to piracy and privateers at sea back in the 1600s to 1800s, and it's a great privates individual criminal actors versus privateers, state-linked groups that give you a little bit of deniability. That's like the example between classic cyber crime versus some of these more state-linked efforts and patriotic hackers.

But in either case, both on the naval side, it's by going after the markets, going after the structures, that's how you dealt with it rather than trying to chase each and every individual one.

This leads to the ISP question. It's a perfect illustration also of how, by going after these structures that everybody agrees are bad, these black markets, it may even give you space for international cooperation where you don't think it's possible. So, as an example, the U.S. Navy and the British Navy, throughout the 1800s, you know, trained to fight each other because, guess what, they had fought two wars against each other. But they also cooperated in anti-piracy campaigns, much like the U.S. and China in this space where there's a lot of issue for conflict and some very real bad things happening, but there's also areas that we could work together against what the Chinese call double crimes, and part of this is also facing the fact that we Americans, we've got some issues.

So, ISPs, one study showed that 20 out of the top 50 sort of cyber crime spewing ISPs are American ones.

The chip question, absolutely, this is a hardware vulnerability that could be baked into our systems and I would just point, to give a military example, it just was revealed that the F-35 program allowed certain chips made in China to be put -- we dropped the waivers around them -- some very deep concerns about what you might call a hardware attack.

MR. FRIEDMAN: So, I think these examples, very quickly, really capture how you need to understand -- you cannot address this issue without understanding the technical, the economic, and the political side of them. So, for example, on the ISP side, different countries have really looked into the options of, should the ISP tell me whether my computer is part of an international botnet that might be attacking Estonia? And the challenge there is on the technical side, we actually don't know very much about what the likelihood of detection is and how it'll respond, what is the probability of re-infection?

If I tell you and you clean yourself up, if you're going to be re-infected immediately, then that's a waste of money and effort.

On the black market side, I think this is a great example, and we're starting some work on that at GW where the focus really is really understanding what technical questions shape the effect of the market. For example, if I discover vulnerability in a major piece of software, what is the likelihood that you as an adversary will rediscover that vulnerability? Because if we're both going to find it, we're going to have very different equilibria in that market and we're going to have very different policy solutions than if the chances of rediscovery are zero.

And so, we need to understand the technical details, how code is secured over time, as well as the market side, and then that will lead us to understanding the governance side.

MR. SHACHTMAN: We've got time for one last question then we'll roll into our last panel. Let's take it here, the black and the blue shirt.

MR. HENSER: Hi. Russ Henser, I'm an attorney in town also.

So, my question is about resources and I'm thinking of the post-9/11 era when in addition to talk about major attacks, there was a lot of talk about hardening up soft targets and what do we do to stop people from going into shopping malls and movie theaters and hospitals and shooting or blowing themselves up. And I think that debate wound up with us deciding, you know what, there's not that much we can actually do to harden those targets, and we've been very fortunate that we haven't seen attacks, or many attacks, but there could be.

Here, it seems to me, if this is a good analogy, the problem is that there's a lot of temptation to those soft targets. Someone who wants my credit card can get it from Target, but they could also get it from the cupcake store or Amazon.com, and I'm wondering, do we have the resources to harden all the soft targets that we need to? And if we don't, what does that mean if people can just find the weakest link?

MR. SINGER: I'll jump in on an example of the military implication of this, and please weigh in.

To me what's fascinating about this is, you know, how we've approached security within DoD, which is, you know, harden the DoD, try and de-link it from these threats, which as we talked about before, hasn't proved possible, both because of threats coming in and just massive amounts coming out, to try to incentivize one part of the Defense economy, the major contractors to get much better at their security. And they have because they've seen these kinds of threats to their intellectual property happening, but then not facing the fact that there's this wider set of targets out there that are quite soft because the incentives are not right, the awareness is not there, that could have just as much implication.

So, to give an illustration, the first book that I did was on private military contractors, how our entire logistic system is dependent on these companies. So, great, you have a perfectly -- let's imagine you have a perfectly hardened, safe, secure U.S. military network, but what happens when someone enters into the logistics company and changes the barcode numbers for the shipment of gasoline to toilet paper? So, you've got that unit out there that gets a delivery from the supply train and it's toilet paper, not gasoline or ammunition. Or if we're thinking about defense industry, the big primes have paid a lot of attention to getting themselves secure, but the supply chain of all the mids, and particularly the small companies, aren't well protected, and that's where we're going in.

And so it circles back to what we were talking about before of understanding that we're all in this space and we need to raise the level of resilience and awareness in it.

MR. FRIEDMAN: And just very quickly on the private sector side, I've been doing the economics of information security for over a decade now and it comes down to two things that we're still trying to understand but we're working towards, one is just how do we think about return on investment, how do we create incentives by saying, listen, if you make yourself more secure, it will be in your interest. And we need a way to communicate that and think about governance parts as well.

And the second thing is just scale. Ultimately, defense comes down to making it cheaper to defend than to attack. And that means we need to raise the cost to the attacker and lower the cost to the defender, and that's a technical question, but that's also an organizational question, it's an economic question, and it fundamentally, as Peter said, is a question of politics and governance.

MR. SHACHTMAN: So, that's all we've got time for with this panel. I want you to join me in giving a round of applause for Peter and Allan.

They're going to be signing books at the end of our next panel outside here. It's also available at cybersecuritybook.com. And now I'd like to ask the second group of panelists to come up to the podium, ask you all to sit tight, and we'll roll right into our next panel.

MR. SINGER: Thank you.

MR. FRIEDMAN: Thank you all.

MR. SHACHTMAN: So Peter asked me to put together this second panel of reporters, and so I just went ahead and picked four of my favorite reporters who not only are great on this issue but are great, you know, just great in general. And so I'll start going -- and fabulous people. Great cooks.

So starting right here to my immediate left, Siobhan Gorman, who is reporter with The Wall Street Journal; David Sanger, whose title is chief Washington correspondent. Is that right now?

MR. SANGER: National security correspondent.

MR. SHACHTMAN: That, too, of The New York Times.

Tom Gjelten of National Public Radio. And in the awesome shoes we have, from the U.K., as you can tell by those shoes, James Ball from The Guardian.

Guys, let's just start with the NSA stuff since it is the big issue right now. Can we talk a little bit about how the introduction of these Snowden leaks has kind of changed the way we're doing business and how much harder or easier it has been to report on the NSA and on the intelligence community as a result of them?

Siobhan, you've been covering the NSA for --

MS. GORMAN: Too long.

MR. SHACHTMAN: -- too long. Yeah.

MS. GORMAN: You know, I think it's actually kind of cut both ways. You know, I haven't been writing so much on the Snowden documents themselves, but I have been writing on sort of related NSA issues in the midst of all of the Snowden revelations. And I've actually found that as many people might feel a little bit less inclined to want to share information about it, there are probably at least as many at this point that now feel -- I don't know if it's emboldened or they just feel that this is an issue that's going to get more attention now and so it's worth their while to, you know, share what they know with reporters, whether it's by way of context or additional information and details. I mean, I think probably on balance it's led to, you know, a greater amount of information that reporters are learning even beyond the Snowden documents.

And in addition to that, obviously, the government is behaving somewhat differently from the way that it did. I mean, NSA setting up a whole press task force to deal with the Snowden leaks. I mean, that's a fairly unprecedented thing for them to do and one can obviously argue that, you know, they haven't been as forthcoming as they should. But certainly, if you're looking at what their baseline was, it's a lot more than it was. And I've also just found it pretty fascinating that the government itself, the director of National Intelligence, has released these huge documents dumps in waves, and especially in the beginning, but even some of the recent ones, we've seen a lot of highly revelatory court opinions from the Foreign Intelligence Surveillance Court that in a lot of ways were more condemning of NSA practices than anything that Snowden put out. So I don't think it kind of cuts one way or the other.

MR. SANGER: I would agree with that. I would add that, pardon me, I think there are three different elements of this to think about. The first is that even before the Snowden leaks happened, I think all of us would say that reporting on these topics has not been easy in Washington. I could recite for you all of the statistics about the number of leak investigations underway by this administration, including against many people on this panel or based on stories that they wrote. But even beyond that, these topics have all been topics on which the Obama administration, I've found, has been sort of less willing to discuss than even the Bush administration. And as we all recall, the Bush administration didn't exactly win a reputation as a fount of openness. So that's the first.

The second is that the immediate response to the Snowden revelations I think was for many of the intelligence agencies to sort of hunker down and not answer any questions, and then they discovered come the fall that that was getting them probably into more difficulty than if they actually came out and explained some of these programs. And what has struck me about the documents that Siobhan has mentioned have come out in recent times is it's reasonable to ask the question "did all of these programs need to be classified to begin with?" For example, had -- and I don't know the answer to this, but I'm posing it as a question -- had the NSA revealed the bulk collection of metadata program, would it have truly helped any terror group that was trying to evade it? Or could they have won some democratic buy-in to this concept, particularly in the years immediately after 9/11?

And I think the third element that's come out is what we've learned from the documents themselves. Many of them have been very revelatory. Some of them have been quite dated. And so you have to avoid the temptation of looking at a document and assuming that just because you're looking at it now it represents what events are like today. And you have to -- so we're at a point with the documents where I think two things have gone on. First, for our general reading public it's become something of a blur. There have been so many documents out there that can't quite sort out what's new and what's not. And secondly, we're at the point where you really have to supplement them with some form of other reporting to be able to explain them.

MR. GJELTEN: I have found this to be a really difficult story to cover in many ways. First of all, the complexity of it. And this, of course, applies especially to a radio reporter who needs to sort of tell people stories and not just sort of write it out and give the opportunity to read the story three or four times before you can get it. You have to get it the first time when I tell it to you. These are some really complicated issues that we're learning about. So just from that point of view it's extremely difficult. I think that there actually has been -- there have been sort of as many errors in reporting this story as I've seen in a while, and I think that's partly because of the difficulty of understanding what it is that we're learning and communicating it.

And then added to that, I don't recall. I've been covering national security for a number of years and I'm curious how the rest of you feel about this. I don't recall a story where there's been as much polarization as there is in this story. Peter Baker David's colleague at the time had a piece over the weekend where he quoted Pierce Wyer, who is one of the members of the president's review group, saying that he had a friend in Silicon Valley saying that 90 percent of the people in his tech company were convinced that Edward Snowden was a whistleblower and that every single person he talked to in the national security establishment felt that Edward Snowden was a traitor. And I think that we have seen this very deep polarization, you know, throughout the way that we've reacted to these disclosures. I mean, it's not that we should, as journalists, shy away from stories where there's a polarization of opinion, but in this case, you know, because we as news organizations, and The Guardian and the Post as well, have been players actually in this story, and you know, there's been a lot of -- it's been a situation where you sort of as a news organization, you have to almost decide what kind of posture you're going to take in approaching these disclosures. So for all of those reasons -- I mean, none of these, as I say, are issues that we should be afraid of dealing with, but it is a really complicated story to report.

MR. BALL: I think it's quite easy to understate the complexity of it if you are one of the sort of outlets with actual access to the documents, and obviously, The Guardian has access to a substantial number of them and we've been doing that primary reporting. I think initially there was this impression that, you know, Edward Snowden was turning over two or three at a time and explaining the way through that, and actually much more his approach was to trust reporters and to trust outlets -- The Post, The Guardian, and various other places that subsequently had been included -- to actually find out for themselves and decide for themselves what was of interest and how to structure it. And that's the extraordinary challenge. There were very, very few of them that were here is this one document and it's brilliant. And they were obviously the ones that went out in the first week or two. The Verizon document now seems like an extraordinarily simple story compared to say some of the ones that touched much more on cybersecurity that we talked about where you're trying to build up this impression. I mean, you start to see very clear signs that there were deliberate efforts sort of not to improve security but to keep it weak because of these issues of everyone using the same systems and the NSA having enough confidence that they could find and take advantage of vulnerabilities better than other people so they would keep those vulnerabilities there or even bake them in. That starts with you seeing a few documents that touch on it a lot and then touching on dozens more and dozens more, and what happens is you have reporters who are diplomatic correspondents who are very good as to the international relations aspect. You have reporters with a more technical background who are trying to sort of separate which acronyms are program names and which are technical acronyms, which some reporters looking at this stuff can't do. You're not looking at a guide. It's not a tutorial. Everyone else knows all the lingo, so you'll have a sentence which means absolutely nothing to any sane human being but it's perfectly comprehensible to anyone who knows about national security.

And so you have the challenges of that, but I think sort of what the reporting has done is it's let us challenge the priors. I think especially on cybersecurity on all sorts of intelligence issues, there's been this sort of decade or more where there's just been a consensus if we need more security, we need more spending, we need more powers. And what the Snowden sort of files did was give a chance to get this democratic accountability, to get this public debate. I think America has actually seized it quite well; Britain, not so much. You know, as you may have noticed, we had a few issues over there and I think, you know, that's fairly commendable. And I think whatever your stance on it, I think the debate can be quite constructive. And I think quite an alarming moment, even if you're not someone who believes Snowden is a whistleblower, as I do, is there was a very strange moment in the U.K.'s Intelligence Committee where the head of MI5 was asked to assess the chances of anything like Snowden happening to the U.K.'s intelligence services, and he blithely, in one sentence, dismissed it. Just said, "Not a risk," as if it couldn't happen. And of course, it already had. There are lots of GCHQ documents in amongst this material. The fact that he seemed to have considered this a black swan (inaudible) should terrify you. I mean, he just evidently didn't understand the question, let alone the risk. And so I think whatever your stance, whatever you think should be done in these areas, it's clear there are a lot of questions still to ask.

MR. SHACHTMAN: It seems like a hallmark of cybersecurity reporting over the years has been the desire by government agencies, by outside contractors, to always heighten the risk. Right? The sky is always about to fall. It's amazing how like every minute of every day the sky is always about to fall. Do these documents change that at all? You know, you talked about all of a sudden, you know, a high-ranking intelligence official kind of lowballing risks. So have we finally seen the end of fear, uncertainty, and doubt, and FUD, or is this just -- how does this stuff changed it at all?

MS. GORMAN: Do you mean in terms of hyping the cyber threat itself?

MR. SHACHTMAN: Yeah.

MS. GORMAN: Like the discussion earlier about, you know, (inaudible) still has not had a big meltdown or something?

MR. SHACHTMAN: Yeah, and also the risks associated, yeah, with these leaks.

MS. GORMAN: Well, it seems like it suggested the insider threat is higher than estimated and the outsider threat may well be lower than estimated. I mean, it also probably shows that maybe making these estimates is not the wisest thing one can do. I mean, the concern, and this is really pre-Snowden but I don't think it's affected by the Snowden documents -- the concern that I would hear particularly from government types or computer security types is not so much that it was high risk but that so many of these cyber attacks could be high consequence. I mean, I think NSA probably feels that their cyber breach, so to speak, was pretty high consequence. So, and in a way the Snowden revelations sort of show how one individual -- I mean, this is asymmetric, you know, an asymmetric conflict or challenge, and so in a way it sort of could actually prove that point, that you don't need a lot of examples to show that it's a big deal. You kind of only need one. The security experts who I would talk to who kind of point to the more traditional threats, you know, this could be like a cyber Pearl Harbor and this, that, and the other thing, is not so much saying the countries or the organizations with the greatest capability, like China and Russia, are going to do it, but more that there's such a burgeoning black market out there that it's only a matter of time until those kinds of things get into the wrong hands, and therefore, you have a reasonable risk of it just getting into the hands of someone who wants to do something bad. I think it remains fairly amorphous, although, like I said, insider threat I think is probably a little higher risk.

MR. SHACHTMAN: Anybody else want to tackle that?

MR. SANGER: The only point I'd make here is that, you know, we now know that one of the reasons that the U.S. government is so concerned about say infrastructure attacks in the United States is that these documents underscore what we knew even before these documents came out, which is that the U.S. has found it's not all that difficult to do some of these things elsewhere. And so that underscores their understanding of the risk to the U.S.

MR. GJELTEN: For me, a big revelation had nothing to do with the Snowden disclosure as it was the story last week of the merger of FireEye and Mandiant.

And reading the bottom line analysis of the revenue of Mandiant and the revenue projections and the stock price projections for this company, I think that was something rarely -- it was important for me to take into account because Mandiant among other cybersecurity forms has been, you know, a really important source of information to us as cybersecurity reporters about the threat out there. And when you read about how much money Mandiant and now Mandiant and FireEye are making, you know, convincing companies and organizations that they are under threat and then proposing ways for them to mitigate that threat, you know, it makes us, I think as reporters, want to think twice about this issue that came up before about hyping the threat because there are some really big financial stakes involved in this debate.

MR. BALL: I think that touches on the absolute core issue as reporters in this particular sphere. Almost all of the incentives are with people to hype up the threat. It's, you know, firstly no one in defense wants to say this is very low risk, this is quite safe. You don't know what's going to happen in the next 12 months, the next two years, but also, you're trying to defend quite large budgets, and budgets often which don't have the same degree of accountability as other areas. You want to stress the dangers. There's a huge sort of private industry that's struggling with defense budgets which aren't going up like they used to. Security budgets which aren't going up like they used to. Cyber is this nice little area which is still a growth area, still a potential. You know, if you read the annual reports of big defense companies, just cyber companies everywhere, this is where they are hoping to keep growth or at least stall shrinking.

And so look at the money, the lobbying money spent in this town on cyber in the last five years. It has gone up spectacularly. I mean, you're talking four or fivefold, and this is still -- the annual rate of growth is huge. There is not much money in saying, actually, hang on. Let's calm down for a bit. Maybe we should do something about squirrels. You know, there's not the money in that. You know, a few people will push it on the civil liberties front. There's not many people going, hang on. You know, we're looking to try and fix deficit. We're looking to try and do this stuff. Should we really be spending this much money on cyber? How do we judge what a win is like? How much responsibility should the federal government be taking for it? Should we leave it more to banks? Should we try and spread the load internationally? There's not really a sort of boring common sense lobby sitting in the middle of this going, "Hang on. You know, maybe it ain't that bad." And so maybe, you know, my position is maybe we have to be more skeptical in the cyber field than in the rest of it. And that's always difficult for journalists because if you go to a news desk saying, "Hey, I've got this great story about a terrible threat," you're much more likely to get a A1 than if you go, "You know, maybe we should just tell people to chill out a bit." It doesn't get on the front quite so often.

MR. SHACHTMAN: I guess I meant on the inversion of the FUD, of the fear, uncertainty, and doubt, is that you've got the NSA and these other operations now saying no, no, no, no. The core cryptographic algorithms are actually totally secure. You know, we didn't really undermine them. Don't worry, these documents, they don't really say what they mean in a way that usually these are the guys that are saying the sky is about to fall and now they're saying actually it's totally fine. So to me I found that interesting.

I'm going to ask one semi-unrelated question and then I want to open it up to the audience. And I guess this is like, are these documents, are they actually just the shiny object that we're chasing and that we're being distracted from like real bigger issues in this space? Or is the big issue itself the NSA, you know, how vast its spying network is?

MS. GORMAN: I guess to me I feel like there's been sort of a sub-story that's gotten less attention and I kind of referenced it earlier when I talked about the documents that have been released by the director of National Intelligence, the FISA court documents. I actually think that there's quite a lot of questions now to be asked about NSA's overall competency. I mean, they seem to mismanage all of these large programs. So, you know, it's kind of this weird double story that we're hearing that it is sort of, you know, omnipotent but it's also kind of incompetent. And so I don't know which makes a civil libertarian feel better, but you know, it's not -- I think it's a little bit more of a nuanced story than just they're taking everything because they're not exactly doing that. And, you know, what we've seen is, you know, when they were attempting to do the phone call records they claimed that they had all these protections. They didn't understand their own program well enough to actually enforce the rules they had promised the court that they would. And we've seen that. We saw that with the Internet metadata collection. We saw that even in tapping the Internet backbone. All of a sudden they're scooping up tens of thousands of wholly domestic communications they swore to the court that they wouldn't take. So I do think -- to me it's just raised broader questions of considering that so many of these programs have kind of perpetuated themselves now for a decade, you know, as these technologies change, how much sort of more coloring outside the lines does NSA find itself doing just by accident and the fact that it doesn't necessarily understand the implications of changes in technology. And what sort of bearing does that have on all the other programs we don't know about?

MR. SHACHTMAN: I'm struck by two elements of this that go to the question of how effective these programs are. If you look at one of the programs they abandoned in 2011, which was the e-mail metadata program, they were looking at roughly 1 percent of all the e-mails sent in the United States, which is a lot of e-mails when you think about it. And ultimately dropped the program in part because of critiques of it internally, but in part because they weren't getting very much out of it. Then you go to the Presidential Advisory Committee report that came out the week before Christmas and they were a lot less convinced about what the metadata program had actually yielded in the way of preventing terrorist attacks than you would get if you were just listening to the congressional testimony of General Clapper and General Alexander.

So even if you consider them to be highly competent and highly good at what they do, and I think for some of these programs they're probably better than any other intelligence agency that we've seen around the world, there's still the reasonable question is the amount of time, effort, money, and in this case, diplomatic and business cost of this worth what you're getting out of it?

MR. GJELTEN: I can say that the amount of time that I have spent chasing NSA surveillance stories and Edward Snowden stories over the last six months has been vastly in excess of what I really would have preferred to spend my time reporting on. Does that mean that it's a bright, shiny object that doesn't warrant the attention we're getting? I'm not sure. I think David's -- I think what the review group said about the effect of this, of these programs, is extremely important given that, for example, Michael Murrell, former deputy director of the CIA, former acting director of the CIA, was on that review group. And I think there is real reason to question some of the more extreme claims made by General Alexander, General Clapper in this regard.

However, I do think that there is -- I think that these disclosures have raised a couple of issues that are hugely, hugely important and really warrant all the attention that they've gotten. And it's not just the tradeoff between national security and civil liberties, which is a debate we've been having in this country for many, many years, but particularly for purposes of this discussion today, it's the tradeoff between the advantages of protecting the good guys versus going after bad guys. And I think that we've seen the tradeoffs in that regard come out really clearly in these documents. The way that the NSA has undermined cybersecurity and has, you know, we've learned a lot about the vulnerability market in the last few months and the way that the NSA has actually held onto vulnerabilities for offensive war purposes, offensive cyberwar purposes, versus sort of the helplessness of organizations like the Department of Homeland Security which you get the feeling that they've been completely in the dark all this time about what kind of offensive capabilities the country has. And it really does seem to direct something that Peter and Allan mentioned earlier. It really does seem that all the priority in this government has been on offensive cyber capabilities really to the expense of cyber defense capabilities. And that's a hugely important issue, and I think that's something that has really been revealed as a result of some of these disclosures.

MR. BALL: I think maybe the most extraordinary sort of competence issue right in the whole thing was right in foreign policy, and it was this brilliant sort of tale from an anonymous CIA official of Alexander coming in and sort of internally promoting the metadata program and sort of bringing in this vast printed out sort of network diagram talking about how you could use it to find the key notes and the people who were keeping different sort of suspects in contact. And he pointed out a couple of things where hundreds of people had been contacting this one number and saying, see, look what we're doing to identify these. And the CIA, I must say, after he goes, so we just decided out of curiosity to take a look at that number. And it was a pizza parlor, which a lot of people call. This is, you know, Alexander, who is regarded as actually one of the more tech savvy, nerdish advocates who knows what he's talking about, relatively speaking, for sort of senior military intelligence officials. And his big case just completely fell internally and it's just one of those concerning fragments that you get.

It makes you wonder sort of the extent to which these kind of large-scale trolls that we really sort of struggled to see much evidence in terms of results to justify have distracted from other missions and this kind of "collect it all" vast ambition has undermined other goals. I think, you know, the obvious threat for cybersecurity is this undermining of (inaudible) security things. There's a more subtle one which is maybe worse, which has to do this combination of intelligence and security coming together and being run by the same agency and the same people. Sometimes that can have some good things. If you're sitting in bits of the backbone of the Internet and the switches and routers, you can see floods of traffic sometimes when they're coming in. It can help you get an early warning on denial of service attacks or that kind of stuff. And we're seeing things suggesting that happens. But if you're trying to persuade companies to let you into their systems to help you defend them, if you're trying to encourage foreign governments to cooperate with you on security and so on while also using cybersecurity as a front for intelligence operations, you are absolutely undermining trust in your companies, in your agencies, in all of the defensive steps you can take. And that kind of overreach is not easily fixed because that's all about your relationships with the tech sector, with your allies, with everyone. And so when will, you know, the U.K. government, the German government, other people who should be working and cooperating, foreign banks, you know, frankly, the World Bank, the U.N., the E.U., when will they actually take advice from a U.S. security agency or intelligence agency on cybersecurity again? It's not going to happen soon. And that leaves us all in a bit of a mess. And so it's actually the issues where there aren't even just the technical side; it's the political mess that's been made of combining intelligence and security and then just vastly overreaching.

MR. SHACHTMAN: That's a really good point because I think people don't quite understand that really the Internet moves because of a series of handshake agreements. Right?

MR. BALL: Yep.

MR. SHACHTMAN: And that there's not a lot of formal documents. There's not a lot of contracts that guarantee that my traffic can make its way to Japan or what have you. It's really just a series of trust arrangements. And if you undermine those trust arrangements, you're really undermining the core of the Internet itself.

MR. SANGER: Which is why this may be the first spy scandal in modern history that's got a bigger business effect than it does diplomatic effect.

MR. SHACHTMAN: Right.

I'm going to open the questions up to the audience, but since this is Peter and Allan's book coming out party, I want to give them the privilege of asking the first question.

MR. SINGER: Hi. Pete Singer, co-author of a new book out that you can find out more about at cybersecuritybook.com.

What I love about the structure of it is the first panel we tried to wrestle with whatever everyone needs to know, and you've been exploring how we report it, how we talk about it. And so I wanted first to thank all of you for coming. I really, deeply appreciate it. And I wanted to pull that thread a little bit further. How do you see news organizations and what's neat is you're from different types -- you know, newspaper, radio, et cetera. How do you see them organizing around the topic of reporting on cybersecurity questions in the future? Do you see that evolving?

And then second, the training for journalists themselves. I mean, you talked about sort of the technical side of reporting on these stories, but also one of the things that's interesting to me is that news outlets have been among the most notable targets of cybersecurity threats, be they from state organizations, you know, a certain large Asian power that shalt not be named, to recently a Syrian electronic army which is not an army but has been having a lot of fun with different news outlets from noteworthy ones to The Onion. I mean, how do you see the training for journalism evolving on this as well as the organization?

MS. BALL: I tend to find, especially in British journalism, there's two things journalists don't like, and it's computers and math. And, you know, anything around this area seems to involve both.

I think this actually, you know, it's a bit of a team effort. I think journalists actually have to start taking it seriously. You know, we've talked about source protection since the dawn of everything, and it's the most tedious truism of the profession, that you would go to prison rather than reveal a source and so on. The problem is now you can very easily reveal a source by accident just because you're rubbish at computers or your Gmail password is 123456. And we have to get better at that. We have to do it quickly. We have to take it seriously. But I think that's kind of become a consensus now. I think part of what else we have to do is start making encryption technology and secure technology and source protection technologies that are actually usable by regular humans because a lot of these systems are very complicated, even if you think personally they're important and are IT literate and savvy. What you tend to find, however brilliant someone is at computer security, if you look at how the hacking groups get caught, if you look at what goes wrong with most things, it's not often that someone didn't have the right system; it's the 3 o'clock in the morning when you've been awake for 20 hours, you desperately have to send a communication, you know, the servers that are meant to hold your encrypted channel aren't working, you give up and you send an e-mail or you just can't face the hassle barrier each time you've got to get in touch with someone and doing what you have to do. The technology has to get easier and has to start to be made with regular, normal, fallible human beings in mind. I think that's sort of the key thing in protecting a news room.

I think we also have to learn to prioritize. If you get in my Twitter account, you will embarrass me, especially if you paste a couple of, you know, tawdry jokes or something, the DM or something like that. But you won't do much more. If you get in my e-mail account, you might find a couple of low level sources who shared a bit of gossip. You won't completely screw me if you get in either. And so I've got to factor and I've got all the things you should do, but I don't lose sleep over the idea of people getting in there. And I think we learn what to protect and what not to, and that way we have enough hours in the day.

After reporting it, I think it's all about team approaches. You know, I think if you have a cybersecurity reporter, I can see why you would have done it for the last few years. I think now that's a big dated. Get people who understand the broader things and get them to work together. People who understand the tech, people who understand the politics. You know, I think journalism works better when we work in teams.

MR. GJELTEN: We just learned today at NPR that we're going to two-factor authentication in our own system, which I would say is probably a direct result of the lessons we've learned over the last few months.

I'm in the National Security Unit at NPR. Up until recently, almost all my collaboration as a reporter was with the foreign desk and the Washington desk. And since I've been covering this story it's been almost all with the technology reporters, and I've just become really dependent on them to help me figure stuff out. You mentioned the -- we're working on a series now about sort of the arms race, the digital arms race between the NSA and the tech companies, and I'm completely dependent on, you know, when it comes time to talk about, you know, end-to-end encryption and security measures, you know, I really depend on our technology people -- technology reporters, and even the technology people at NPR to help me with this. So it is for us, just in our own case, it has really opened up whole new sort of areas of collaboration that really weren't there before.

MR. SANGER: Well, Peter was right that The Times has been the target of two different -- at least two different big groups. There was a Chinese group that came in and lived in our computer systems for several months back in 2012, we think searching for the sources of stories about how the prime minister of China's family got so wealthy while he was prime minister. And they did a remarkable job of finding their way around a computer system that has stymied me for decades. So I was impressed.

And then we've had the Syrian electronic army, less sophisticated, come in and attack. One day last summer, I think they actually managed to close down the website for a good part of the day, and the paper came up with a very innovative response, which was we took all the stories we had written that day and we printed them on paper and then we drove around different parts of the country and dropped them on people's doorsteps. Remarkable, technological approach. That was Gutenberg's best day in decades. So.

But within the paper itself, we're pretty accustomed to having collaborations that move between the technology and the foreign policy and domestic policy side. I worked for years with Bill Broad in our Science Department and we did the A.Q. Khan nuclear proliferation stories together. I've worked for years with John Markoff, one of our best Silicon Valley reporters, and we did much of the early Stuxnet Olympic Games reporting that way. But it's always a challenge internally because you have to cross bureaucratic barriers within a news organization. But I think that more and more news organizations have discovered the necessity of that, and it's no longer really a choice. If you tried to do an analogy to a previous era, it wouldn't have made sense in the 1940s and 1950s to just have a submarine reporter or just have a reporter covering nuclear weapons when they were coming out. Ultimately, while you wrote a lot about those, that had to get integrated into a broader national strategy. And I think the argument all of us have been making internally I suspect is this reporting more than anything needs to be put into a broader national strategy and I think Snowden has helped with that. You made the point that in Britain it's been hard to get much of a debate. I thought after many of the revelations about the U.S. participation in developing cyber weapons there would be the kind of debate in the U.S. about cyber weapons that there was about drones. But that's taken longer to generate. So these things are hard to predict.

MS. GORMAN: Well, in terms of how The Journal handles cybersecurity, I've sort of witnessed the evolution because I came to The Journal in 2007 and I had been covering NSA quite a bit when I was at The Baltimore Sun. And so I came in and I had actually just done a larger story on this effort that we later learned was the Comprehensive National Cybersecurity Initiative. I spent a year trying to get our editors to care at all about cybersecurity. They kept saying, well, who is being hurt? Is this real? Does it involve people? And, you know, like, bring me examples and find me the company, the company that admits to being hacked. And this is 2008, there weren't a lot of those.

And so somehow in 2009, we were able to kind of shake loose a few stories that got, especially our editor's attention really, and they were won over and we did a little bit too good of a job because then all of a sudden it was like every single -- and I cover intelligence, so, you know, cyber is part of it but it's not the whole thing. And I had sort of just had this internal lobbying campaign thinking like this would be a cool set of stories to do. And so it's been kind of interesting because all of a sudden in 2009, like I was supposed to do every hacking thing ever in addition to my regular job. And over time I think it kind of started a little bit more with like the banking and financial reporters, that they realized that this was a story that their companies really cared about. And so little by little over the last, you know, few years really, different reporters who are responsible for different sectors -- you know, energy and what have you -- have kind of taken their own interest in it and we'll work together when it's relevant or not. But, you know, The Journal, I think, was probably a little late to the party in that it was only last year that we actually started a dedicated cybersecurity -- added a dedicated cybersecurity reporter which isn't necessarily just to make sure that cyber is this person's problem but almost to make sure that they can kind of traffic cop those issues and this is someone who he was in D.C. and he's now based out in San Francisco, but, you know, can kind of do it, especially from the corporate side and kind of recognizing that this is at least as much a corporate story as it is a national security story. So the way that we break it down at this point is I handle some, but not all of the national security stuff. He does a lot of the corporate stuff, and we all kind of work with our colleagues.

In terms of sort of reporters' own cybersecurity, I mean, like The Times, The Journal was also hacked. And reporting that story was actually quite an interesting phenomenon. I think it was rather different from what David experienced because when his story went up I heard from my editor, "Well, wait a second." This was like 10 o'clock at night. You know, "Wait a second. You don't need to do anything with it yet. We may have our own problem to report." I'm like, "Oh, good." So I'm like waiting for someone to call me at 10:30, like one of our lawyers and explain it. No. Like nothing, nothing,

nothing. And so the next morning I show up in the office and I'm like, "Okay, guys. What are we doing?" And they said, "Well, you can go report the story like any other hack." And I'm like, "Oh, this is great."

So The Journal was not quite so forthcoming. I think it took until 4 o'clock in the afternoon the next day to get this impenetrable statement from our own company that kind of admitted that we had been hacked. So, you know, they claimed that they needed to wait until all of the new security procedures were put in place before they spoke about it. But, you know, it was the kind of thing where, you know, even after that we have to call our own corporate communications people. Can you still give us that assurance that nobody is roaming around in our systems?

So I think what I learned from my experience reporting that particular story was, one, my company wasn't going to necessarily tell me if I had been hacked, not that that was particularly in evidence there but I learned that reporters in our Beijing bureau only heard sort of on the down low that they had been hacked. You know, obviously, it can happen to us and so you take precautions but you also sort of operate under the assumption that it could certainly happen to you.

MR. SHACHTMAN: That's an amazing story.

I'd just say from an editor's point of view, as cybersecurity and other sort of technical issues have become more important to general reporting, there's been a training of reporters it's had to happen to. And reporters that maybe came up in a political milieu that were okay with "he said, she said," and sort of no real right answers. It's like, no, actually, there are right and wrong answers when it comes to technology. There are things that technology can do or can't do, and so I'm thinking of one reporter in particular that took like a year and a half for me to beat that out of him, and it was a process, and now he knows, and I think we're all better for it.

MR. SANGER: Spoken like a true editor.

MS. GORMAN: You backed up to management well.

MR. SHACHTMAN: All of his successes are, of course, all attributable to me.

Let's go -- let's start in the back there. Yes, sir.

MR. BRODSKY: Marc Brodsky, retired CEO in publishing and physics, strange enough.

You talked a little bit about the controversy -- the tradeoff between intelligence and civil liberties. There's also another one that hasn't been mentioned as much, and that's the tradeoff between intelligence and democracy. There's such a thing as a black budget that not many of us know how big it is, how it's set, who makes decisions, and what is democracy if a large fraction of our national budget is made without public debate or public knowledge? Doesn't that issue come to the fore with all the funding for the NSA and what they're doing? And Congress has decided or who has decided whether to fund this? What has happened to the appropriation process?

MR. SHACHTMAN: That's a good question. Who wants to take it?

MR. SANGER: I'll take a first shot.

Even before Snowden happened there was the beginnings of some revelations about the size of the intelligence budget, and then the Snowden revelations themselves included a lot more budget numbers. Now, it turned out that a lot of those budget numbers were wrong, and that actually tells you something about why you've got to be careful about some of these documents. There was one budget document we looked at that I think The Post had written about fairly extensively that indicated that there had been 231 offensive cyberattacks in -- help me here -- 2011, was that it when this came out?

MR. BALL: It was the appropriation for '12-'13.

MR. SANGER: Right. And it turned out later on that the document had been put together by a budgeter who didn't know very much about what an offensive cyberattack looked like. And as we dug further into it, we discovered that most of those were not what people on this stage would call offensive cyberattacks.

So you've got two layers of problem. One is the secrecy around the budgets themselves, some of which is being lifted. And the second is a definitional one that would enable us to understand how much is being spent in a lot of areas where even within the U.S. government there is argument about how you would define them.

MR. BALL: I think it epitomizes a broad problem. I worked on the State Department cables as WikiLeaks released those, and there were some quite serious and quite concerning public interest stories in there. But a lot of what you read in those cables you're thinking these are pretty good public servants. You know, one or two of them could certainly write more nicely than I can, and I meant to be paid for that. You know, they're doing a lot of the private policy goals, but more or less what the U.S. says it does in public. And you think, you know, about two-thirds of the president's job is probably foreign policy and military policy, and the vast majority of it is kept secret. And so I sort of -- the thing that really struck me when we were going through those cables was what's going on with this reflects of secrecy. You know, this is the bulk of what the administration is doing. A lot of it is fairly innocuous. I think the same with these sort of intelligence budgets. You read, you know, the black budget, which was a budget appropriation document amongst the stuff in the Snowden material, and The Washington Post released a fairly significant chunk of it.

If you read that, it's very top line. It's quite broad. You know, there's a lot of stuff in that that can be made public, if not particularly useful information. And it might also just make you think, well, should we be spending $500 million on this particular thing? You know, if nothing else, yes, okay, there's the democratic issues. There's all of those, but are we not also possibly wasting a lot of money that we could do something better with? And so, yes, there is -- when you have that degree of secrecy, you do get mighty democratic issues. They touch them a lot. I mean, you're right.

MR. SHACHTMAN: Let's go here in the second row.

MR. GLUCK: Thank you. My name is Peter Gluck.

Can any of you envision a scenario in which the United States government gets custody of Snowden on American soil? And that could be an embassy in another country, obviously.

MS. GORMAN: I mean, anything is possible. Right? I mean, we haven't, you know, I don't -- I certainly don't know a lot about Snowden's calculations. I don't know that we know a lot about the administration's calculations at this point except for the fact that they seem to have been not totally amenable to the notion of clemency and that sort of thing. I mean, one interesting thing that we will see in the coming year is whether or not that issue sort of gains political momentum and it becomes a real subject of public discourse or whether that's kind of played itself out. I think sort of where he ends up may be as much of a legal decision as a political one.

MR. SANGER: So if President Putin decides it's no longer in his interest to have Snowden as a guest of the state, you could imagine him being placed on an airplane someplace and landing somewhere where he really doesn't want to land.

MR. GJELTEN: I think he's only got permission to be there for one year, so this is not necessarily an issue that's going to be up to Snowden and his lawyers.

MR. BALL: I think the only stance for anyone has to be that we don't know. I wonder whether there is a case that the likelihood of people fleeing the country when they make these kinds of things rather than sort of doing what happened with the Pentagon papers and Dan Ellsberg and all of that. You wonder if perhaps the treatment -- the pretrial treatment of Manning -- Chelsea Manning as she is now, has made it more difficult to convince people actually to stay in the country and trust that the justice system will give them a hearing to decide if they're a whistleblower or a traitor and what the right punishment is. I do wonder if that, especially the pretrial treatment, and also a really quite long sentence given that everyone has acknowledged there is no proven harms come to anyone as a result of what Manning did. I wonder if that particular treatment has made it less likely that in the future the U.S. justice system will get to make these decisions. And maybe that was a mistake.

MR. SHACHTMAN: Over.

MR. DOWNIE: Thank you. Richard Downie from Delphi Strategic Consulting.

You've talked a lot about the NSA, and actually getting somewhat to your point about the difference between the intelligence and whatnot, this morning actually Tom Gjelten was on the Diane Ream Show. Some of you may have heard it, and I was driving. Unfortunately, I heard about only 10 minutes. But in the first salvo, Richard Clarke described the fact that what they were doing with the NSA review panel was -- he said, number one, we've been asked to take a look at what intelligence do we actually need? And second, we've been asked to look at how transparent can we be in getting that intelligence in a way that matches our democratic values in a democratic society? And unfortunately, I didn't hear much more. I heard your first salvo but not much more than that. And I really wonder, given all we've talked about here with this NSA review panel, are we on the right track or is this going to deviate? Maybe I would have found out if I'd heard the rest of the show, but I look forward to hearing your views. Thanks you.

MR. GJELTEN: I actually think that that review panel -- it's a fascinating report. It's one of the things that we talked about. Somebody called in and said that report was very glib, and I responded as someone who actually has to read a lot of government reports, you appreciate one that's written in clear language and easy to understand. I think that was a really important report, and I think that Dick Clarke and Mike Murrell and the others, I think they really did make an effort to sort of be nuanced about this and to be sympathetic to all the concerns that have been raised but also to the national security establishment from which they themselves come. I just think that that was a very interesting report that really set the stage quite properly for precisely the kind of legislative and executive branch action that is probably forthcoming now.

MS. GORMAN: One of the most interesting things about the report was that the group was panned so much in the beginning as being just sort of, you know, a handpicked panel by the administration, and everyone looked at the membership and said, oh, these are all ex-government guys or allies of the administration. And I remember starting to hear rumblings maybe in October or so. Well, you know, these guys are taking a pretty broad look at NSA structure, and I'm thinking, like, is that really their mandate? And you know, you kind of started to hear little rumblings along the way that suggested that they might actually make some recommendations that would get noticed, and I do think that, you know, I don't know whether or not that played a role, that kind of initial doubting or not. But it seems like they certainly took it quite seriously. I mean, my understanding was that the individual members of the panel were spending multiple days a week of their own time on the panel during that time period. So you know, it does seem to have produced something that will really drive a debate and a policy discussion.

MR. GJELTEN: One of the things that Dick Clarke said this morning was that we're in a period, relatively speaking, of peace right now, and this is really an important opportunity for us to think about what we don't want to happen in the future -- this being, you know, the kind of fiasco that we've seen with the NSA. This is the time to come up with some roadblocks to make sure that we don't have these kinds of abuses in the future.

MR. SANGER: You know, I think the word "abuses" is sort of really a central one here because the group was not really asked to come up with the answer to the question "what here is legal?" That will obviously be in the courts. In the past couple of weeks, we've seen court decisions on all sides of this. Eventually, you suspect some of this is going to end up in the hands of the Supreme Court. Instead, the question the president asked them to answer was do we have programs here that we are doing just because we can instead of because we really need them, because we should do them?

That's a very different question because then you get into a cost-benefit analysis of the kind I referred to earlier, which is is the amount of intelligence you're actually gleaning from this: (a) useful, and (b) worth it given the diplomatic cost, the cost to confidence in American companies, whether it's Apple or Google or server manufacturers. And thirdly, is it useful to us diplomatically? I mean, if it's done this kind of damage to our relationships with Germany, Mexico, Brazil, who knows who else is on the list, with things that may be disclosed in the future, you then have to ask yourself a question -- is what you're learning about the internal workings of the Mexican government or the Brazilian government or the Germany government actually worth it for the cost of revelation? And the most remarkable thing I think I learned in the course of this was that while the CIA asked that question very often about covert programs, if it got revealed, would the damage done by worth it? In the case of the NSA, because they didn't believe their programs ever would be revealed, I don't think they asked that question very often.

MR. SHACHTMAN: I've got time for one last question.

MR. MARQUEZ: Richard Marquez, Federal Government.

Thinking about Julian Assange and the WikiLeaks, the counterpoint that year was Zuckerberg, Facebook, social media, redemptive technology story. Is there a counterpoint perhaps to Edward Snowden? It's polarized but is there a figure out there? Is there a technological trend that might say the Internet and cybersecurity has a positive future? We don't have to worry about Balkanization. We don't have to worry about vulnerabilities, state, all the way down to the individual. Is there a counterpoint to this discussion that says positive future for technology and the Internet?

MS. GORMAN: Twitter's IPO.

MR. BALL: I think it's all going to lie in the response. The governance issue is the big one for the next year because almost any development on it would be negative for Internet freedom in areas where it's really important. And I mean, one of the unfortunate things is the U.S. Government has been funding some fairly good Internet freedom programs. Some fairly wasteful ones as well. But there's no trust for them now. There's no space for them. And it's just not going to be taken seriously outside. I think speaking as somebody who isn't American as well, you know, there is this perception that, you know, ICANN is in theory an international institution but it leans American. The actual architecture of the Internet leans American. You know, 90 percent of the traffic tends to traverse the country and the attitude that sort of the government and the intelligence agencies have taken to that has been essentially, well, let's take advantage of it. It's now no longer a given. U.S. dominance of the Internet is no longer a given, and something is going to have to give there. And America can either fight and say, look, we are just the best place to host the Internet, which might even be true. I think it may still be true. Or try to work out how to concede it, go more multi-lateral, find something that works that actually protects what's good about the Internet. But I think it's all about the response of it, and it could go in quite a bad direction. And I think it would be a shame if the result of the exposure of the U.S. abusing its position of influence over the Internet is that it allows other states to start abusing newfound powers over the Internet. I think that's the exact opposite direction to what we want, but it isn't a given yet. And actually, a large degree of what happens next depends on the U.S. response.

MR. SHACHTMAN: Okay. I think we're out of time. Let's give a hand to our panelists. I thought that was super.

(Applause)

MR. SHACHTMAN: Allan and Peter are going to be signing books in the next room over here. And thank everybody for coming.

* * * * *

CERTIFICATE OF NOTARY PUBLIC

I, Carleton J. Anderson, III do hereby certify that the forgoing electronic file when originally transmitted was reduced to text at my direction; that said transcript is a true record of the proceedings therein referenced; that I am neither counsel for, related to, nor employed by any of the parties to the action in which these proceedings were taken; and, furthermore, that I am neither a relative or employee of any attorney or counsel employed by the parties hereto, nor financially or otherwise interested in the outcome of this action.

Carleton J. Anderson, III

(Signature and Seal on File)
Notary Public in and for the Commonwealth of Virginia
Commission No. 351998
Expires: November 30, 2016